



STRATEGIC INTELLIGENCE, RESEARCH AND ANALYTICS

Summary NIRA Vulnerability Profiles: Crowdfunding and Payment Processing Services Providers

BACKGROUND

(U) While Payment Processing Services Providers (PPSPs) and Crowdfunding were not previously subject to reporting obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), they were included in the 2021 National Inherent Risk Assessment in order to assess their money laundering and terrorist activity financing vulnerabilities, given their importance and widespread use within Canada.

(U) This document summarizes the contents of their respective vulnerability profiles found in the National Inherent Risk Assessment. Additionally, it provides a summary of any references to crowdfunding and Payment Processing Services Providers (PPSPs) risks associated with the Ideologically Motivated Violent Extremism (IMVE).

REFERENCES IN DRAFT PUBLIC-FACING 2021 ASSESSMENT

(U) The draft 2021 public-facing report mentions crowdfunding briefly as something FINTRAC has observed in the context of IMVE threat actors receiving payment to their personal accounts as reported in the June 2021 Special Bulletin. Otherwise, it is mentioned only as an area that is assessed for money laundering and terrorist financing (ML/TF) risks, but not currently within the Anti-Money Laundering / Anti-Terrorist Financing (AML/ATF) Regime.

(U) Payment Processors are similarly mentioned in the context of FINTRAC's 2021 Special Bulletin, noting that Canadians may fund international IMVE networks without themselves being members of organized groups and that payment processing companies, as well as money services businesses, were typical used to make such international funds transfers.

(U) IMVE receives a "preliminary assessment", the core of which relates to analysis published in the 2021 FINTRAC Special Bulletin.

VULNERABILITY PROFILE SUMMARIES

CROWDFUNDING

(Prot. B) The overall inherent risk of Crowdfunding in the NIRA was determined to be **MEDIUM**.

- (U) Crowdfunding is the practice of funding a project or venture by raising financial contributions from a number of people, typically through online platforms, in order to be able to carry out a project, investment or other endeavor requiring funds.
- (U) Crowdfunding connects like-minded groups of individuals, who may be geographically disparate, to pool their resources and have an outsize effect on their common cause. This is

particularly useful for groups whose numbers may be relatively sparse within a locale, but may instead rely on a national or even global reach.

- (U) [Valuates Reports](#) estimates the crowdfunding industry was worth US\$10.2 billion in 2018 and expected to reach US\$28.8 billion by the end of 2025. The [Conference Board of Canada](#) reports that the Canadian market remains much more oriented toward non-business crowdfunding than business crowdfunding (\$180 million vs. \$50 million in 2016).
- (U) The [Canada Media Fund](#) identified a list of 28 crowdfunding platforms accessible to Canadians in 2018 (11 Canada-based and 17 foreign). The 2019 [National Crowdfunding and Fintech Association \(NCFA\)](#) Directory suggests there may be approximately 111 business registered by the NCFA offering crowdfunding portals (largest portion), equity-based platforms, lending platforms, as well as other related services.
- s.38
-
-
- (Prot. B) Crowdfunding initiatives represent a two-fold money laundering vulnerability:
 - 1) vulnerability for investors to become victims in investment fraud (or fraud in general); and
 - 2) the vulnerability of moving illicit gains already in the financial system through the financial system (layering).
- (Prot. B) Crowdfunding campaigns offer a potential cover for the movement of funds between individuals, can bring legitimacy to a particular cause, help fund a fraudulent cause or help divert funding to a fraudulent spinoff project by deceiving investors.
- (Prot. B) To launder funds through a crowdfunding campaign, various 'donors' may make single or multiple donations of a desired amount to a campaign, which then could be withdrawn and deposited into various accounts.
 - (Prot. B) In more sophisticated money laundering cases, crowdfunding fraud may be combined with various other diversionary tactics to "layer" or "structure" financial transactions in order to disguise the origin and destination of funds, and avoid alerting authorities.
- s.38

s.38 . Illicit crowdfunding campaigns can also be set up to defraud donors. Individuals may fabricate charitable causes entirely, or associate their campaign with a legitimate cause to misdirect donors about the use of their funds.

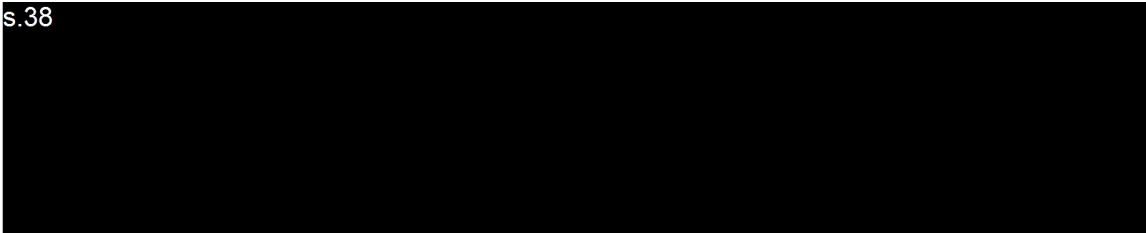
- (Prot. B) Crowdfunding may be vulnerable to wittingly or unwittingly facilitating terrorist activity financing, particularly where the true purpose of the funding campaign is unclear. According to the [Financial Action Task Force](#), crowdfunding and donations represents one of the three main sources of funding for terrorist recruiters, along with support from terrorist organizations and proceeds of criminal activity.
- (U) A [2017 report](#) from the European Commission to the European Parliament identified that while it may not be financially viable to raise or channel large amounts of money through these means, individual terrorists often have minimal financing requirements that may be achieved by raising small amounts of money, potentially undetected, through crowdfunding. The report also identified the vulnerability level of crowdfunding platforms to be “significant” as there is a lack of harmonized controls and a horizontal framework to deal with crowdfunding.

PAYMENT PROCESSING SERVICE PROVIDER

(Prot. B) The overall inherent risk of Payment Processors in the NIRA was determined to be **HIGH**.

- (U) Payment Processors or PPSPs help merchants accept payments from customers by connecting them to payment networks for the purposes of authorization, clearing and settlement of transactions. They may also provide the technology, hardware, and services that enables the merchant to accept a variety of payment methods, including credit cards, debit cards, digital e-wallets and bank-to-bank.
- (U) There are two main stages to payment processing: the authorization (approving the sale) and the settlement (getting money into the merchant account). Examples of PPSPs operating in Canada include PayPal, Square, Moneris, Chasepaymentech, Payfirma, Stripe, and Bambora.
- (U) A PPSP was only subject to the obligations and requirements outlined in the PCMLTFA when it met the definition of one of the reporting entity sectors, such as a Money Services Business (MSB) or possibly a financial institution.¹ The Economic Emergency Measures Order and associated regulations impose additional obligations on certain reporting entities already subject to the PCMLTFA, and extend these obligations to entities not previously covered, such as crowdfunding platforms and PPSPs.
- (Prot. B) This sector is considered large both in terms of volume of transactions and assets. PPSPs are easily accessible to a number of businesses or people and provide the capability to transfer funds within or outside the sector in Canada and internationally. [Payments Canada](#) reported that in 2017, the total payments market in Canada grew to 21.9 billion transactions worth over \$9.7 trillion.
- (U) Misuse of PPSP is often similar to other layering methods, and [can include](#):

¹ This is prior to the Emergency Economic Measures Order: SOR/2022-22.

- Front companies, which use legitimate businesses to cover for criminal activity.
- Pass-through companies, which give illegal businesses access to a legitimate company's payments processing account to process credit card receipts.
- Funnel accounts, which accept credit card charges from multiple companies that do not have their own merchant payment account because they are either too small or they engage in illicit transactions. The funnel company enters the payments as legitimate transactions to the card payment processing system.
- (U) [Open source reporting](#) on this topic has often referred to "transaction laundering" or "factoring", highlighting the complexity of today's payment system, the number of actors involved in payments, and the speed of the transactions, as factors that enable misuse. Since there is often no face-to-face customer contact when individuals conduct transactions facilitated by PPSPs, there is a certain risk of identity fraud as customers can conceal their true identity and provide inaccurate information to disguise illegal activity.
- s.38 
- (Prot. B) Over the past several years, FINTRAC has noted an increased prevalence of new technologies in its suspicious transaction reports and disclosures of money laundering and terrorist financing activities to law enforcement. Virtual currencies, email money transfers and payment processors in particular have increased in prominence in FINTRAC's reporting.

IMVE INTERSECTIONS WITH CROWDFUNDING AND PPSPS

- (U) Using personal accounts, organized groups largely relied on electronic money transfers and cash deposits for their fundraising activities. These transfers typically involved small amounts. FINTRAC observed several IMVE-related payments to personal accounts from crowdfunding sites.
- (U) FINTRAC assesses that individuals in Canada may fund international IMVE networks, while not necessarily being members of organized groups themselves. These individuals typically used payment-processing companies and money services businesses to make international funds transfers. Financial support to IMVE groups also took the form of one-time donations. While these transactions tended to be small, recurring transfers to multiple nodes of the same international network in different countries, they totaled significant amounts.
- (U) In recent years, online crowdfunding platforms and social media sites have started to crack down on IMVE fundraising and promotional activities. This has led IMVE threat actors to seek alternative outlets. These tend to be smaller platforms than the mainstream ones, and they do not always have the resources to monitor and shut down IMVE activities. In response to

increased restrictions on online platforms, IMVE threat actors have been encouraging their followers to send them money via mail, cheques or money orders.

- (U) Following their de-platforming, IMVE threat actors have also increasingly turned to virtual currencies for fundraising. Threat actors mainly use virtual currency donations to fund their propaganda and recruitment efforts. The use of virtual currency has been associated with only one IMVE attack so far.
- (U) FINTRAC is aware of the growing use of virtual currencies by IMVE threat actors to send and receive funds. However, the individuals conducting transactions with someone in the network of IMVE threat actors were not always IMVE threat actors themselves.
- (U) The continued use of business accounts by IMVE-related actors could enable groups to raise larger amounts of funds under the guise of legitimate business transactions. This is because business transactions are generally larger than those involving personal accounts and can be conducted without raising much suspicion.